



# **Interlink Merchant Triple Data Encryption Standard (TDES) Compliance Webinar**

**Ross Snailer  
Payment System Risk**

**Stoddard Lambertson  
Payment System Risk**

**September 9, 2009**



# Agenda

- Visa PIN Security Compliance Program
- TDES Rational and Policy Overview
- PCI PED Testing Update
- Q and A



# Visa PIN Security Compliance Program



- Ensure the continued protection of acquired interchange PINs with sound key management practices
- Visa's Global PIN Security Program requires **full** compliance with:
  - *PCI PIN Security Requirements*
  - *PCI Encrypting PIN Pad (EPP) Security Requirements*
  - *PCI POS PIN Entry Device Security (PED) Requirements*
- Applicable Visa requirements:
  - All PEDs must be using TDES
  - All attended POS PEDs must be pre-PCI / PCI approved
  - Appendix A – PCI PIN Security Requirements
- Visa conducts regular PIN Security Field reviews of program participants to validate compliance
- Requests annual attestations of program participants
- Provides educational PIN Security trainings

# TDES Rationale



## Business Objectives

- Secure Visa's payment system and maintain consumer confidence
- Ensure continued adequate PIN protection
- New TDES compliance policy balances business impacts with risks to the payment system

## Global Standards no longer recognize Single-DES

- Single-DES (SDES) susceptible to compromise
- Organization for Standardization (ISO) and American National Standards Institute (ANSI) online and off-line retail key management standards no longer reference the use of Single-DES

## Visa established global TDES usage requirements affecting both hardware (PIN-Entry Devices) and Key replacement at:

- All VisaNet Processor connections (host-to-host)
- All ATMs and all POS PIN-Entry Devices

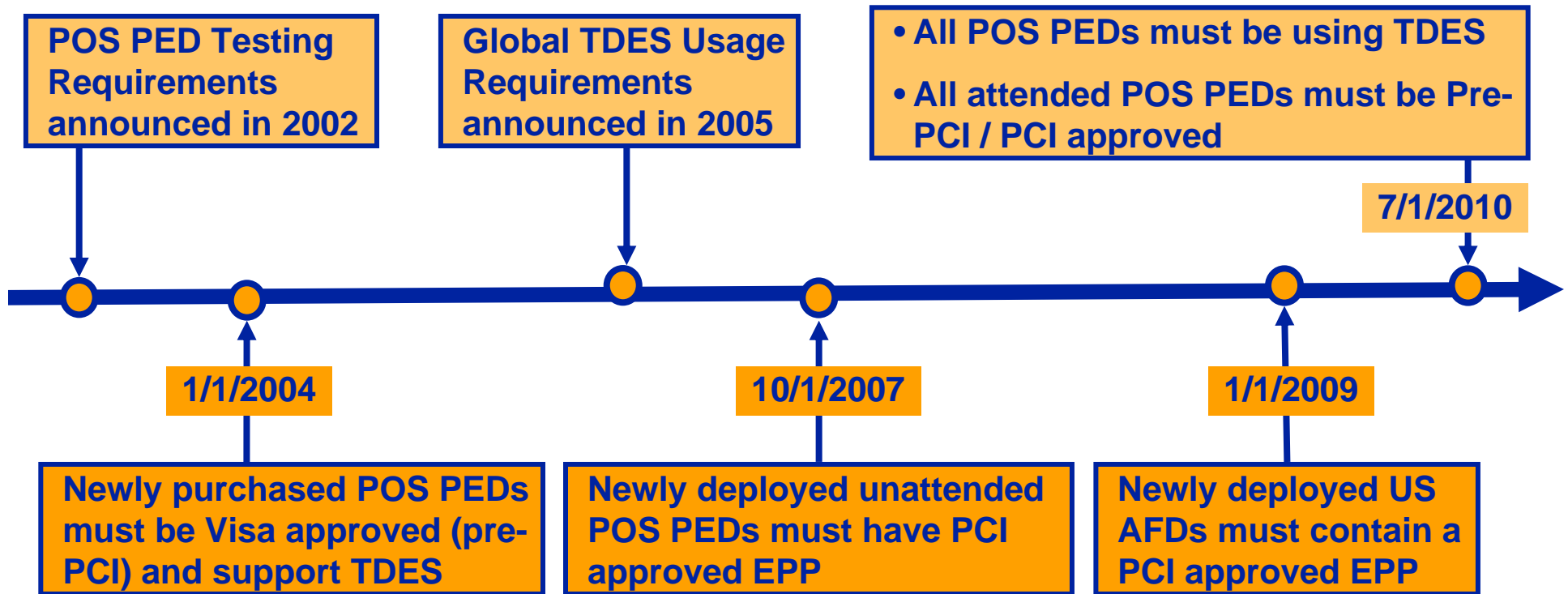
## Visa is the established industry leader as the most secure way to pay

- TDES usage requirements support this promise to cardholders

# POS: TDES Hardware and TDES Usage Mandates



Multiple articles published since 2002 to inform clients



*All US ATMs and VisaNet Endpoints have been using TDES since 2007*

# New Enforcement Policy for POS TDES Usage

## **TDES Enforcement Policy announced April 22, 2009**

- *Visa Business News Article*
- *New Visa TDES Frequently Asked Questions*
- Both available on [www.visa.com/cisp](http://www.visa.com/cisp)

## **Visa will maintain the July 1, 2010, global TDES usage mandate**

- Enforcement policy for TDES usage applies separately to:
  - Attended POS and kiosks -excluding Automated Fuel Dispensers (AFD)
  - U.S. Petroleum Merchants
    - Automated Fuel Dispensers
    - Encrypting PIN Pad (EPP) usage

## **Merchants should check with their Interlink sponsor to determine applicability**

- Visa's TDES messaging began in 2002
- Some merchants have implemented TDES or on target



## **TDES Compliance Policy: Attended POS and Kiosks**

### **POS/Kiosks — TDES Usage (excluding U.S. AFDs)**

- ***Effective October 1, 2009***
  - Sponsoring Interlink acquirers must submit to Visa a summary TDES compliance status report and plan to achieve full compliance for sponsored attended POS and kiosk activity
  - Reports must be submitted to Visa quarterly
  - Reporting template provided to Interlink Acquirers
- ***Effective August 1, 2012***
  - Acquirers may be assessed fines for sponsoring any non-TDES compliant merchants or agents
  - Visa's goal is not to fine clients, but to encourage adoption of TDES



# TDES Compliance Policy: U.S. Petroleum Merchants

## U.S. Petroleum Merchants — TDES Usage

- **Effective October 1, 2009**
  - Acquirers must submit to Visa a TDES compliance status report and plan to achieve full compliance for sponsored AFD activity
  - Reports must be submitted to Visa quarterly
  - Reporting template provided to Interlink Acquirers
- **Effective July 1, 2010**
  - Merchants must be using at least Single-DES (SDES) Derived Unique Key per Transaction (DUKPT) **or** TDES
  - SDES DUKPT widely used but it is **not** the end-state goal – TDES is
  - Requirement implemented to manage risks introduced by (Master/Session) shared key scenarios
  - Visa’s goal is to promote TDES adoption and not fine clients
- **Using information provided in plans, Visa will determine a TDES usage mandate for AFDs**
- Inside petroleum sales (non-AFD) are managed under the POS category





# TDES Compliance Policy: U.S. Petroleum Merchants

## U.S. Petroleum Merchants — EPP Usage

- TDES capable hardware critical to TDES implementation strategy
- U.S. AFD EPP mandate delayed by 5 years
- PCI-approved EPPs for AFDs available since 2008

### ***Effective January 1, 2009***

- Newly deployed AFDs must contain a TDES-capable PCI-approved EPP
- Acquirers may be assessed fines for non-compliance

### ***Effective October 1, 2009***

- Acquirers must submit an AFD EPP attestation for newly deployed AFDs at sponsored merchants
- Reporting template provided to Interlink Acquirers

# Quarterly TDES Reporting



Visa's quarterly TDES reporting requirements are a critical aspect of Visa's compliance strategy and enforcement policy:

- Collaborative effort with Interlink acquirers and Visa
- Allows acquirers and Visa to monitor TDES implementation progress and compliance rates
- Will help establish a reasonable and achievable TDES usage date for U.S. AFDs
- Helps both Visa and Interlink acquirers to pro-actively manage the risks introduced by ongoing SDES usage
- Enforcement policy is based on the current risk environment that exists for cardholder PINs
- Changes to the policy will be based on further analysis of exploited vulnerabilities, emerging risks and threats to the payment system

# SDES PIN Compromise Liability



In the event of a PIN compromise due to the use of SDES past July 1, 2010 acquirers will be subject to:

- Account Data Compromise Recovery (ADCR) and Data Compromise Recovery Solution (DCRS), or similar program liability
  - <http://usa.visa.com/merchants/operations/adcr.html>
- Potential fines if the entity is found to be non-compliant with the *Payment Card Industry PIN Security Requirements* including *any* use of SDES past July 1, 2010

# PCI PIN Entry Device Testing



PCI Security Standards Council (SSC) manages and approves laboratories for testing PEDs and PED approvals

- Visa started program in 2002 (Pre-PCI PEDs)
- Adopted by PCI SSC in 2007

Testing consists of verification of the Hardware, ***Firmware*** and TDES capability

Separate processes for the evaluation of POS and EPP

- [www.pcisecuritystandards.org/pin](http://www.pcisecuritystandards.org/pin)

Visa has set mandates for the use and deployment of PCI-Approved PEDs

# New PCI UPT and PCI HSM Devices



## Visa has set mandates for the use these PCI PEDs:

- *PCI Encrypting PIN Pad (EPP) Security Requirements*
- *PCI POS PIN Entry Device Security (PED) Requirements*

## Visa has not established mandates for the use of these devices:

- *PCI Unattended Payment Terminal (UPT) Security Requirements*
- *PCI Hardware Security Module (HSM) Security Requirements*
- When a significant amount of UPTs and HSMs are approved Visa will establish mandates
- Mandates will not be retroactive but only for newly deployed devices
- UPT is currently a best practice – Use of PCI EPPs in Kiosks and AFDs is mandated by Visa
- See *Visa PED FAQ* on [www.visa.com/cisp](http://www.visa.com/cisp)

# Sunset of Attended Pre-PCI POS PEDs



- **Types of Attended POS PEDs:**
  - PEDs that were never approved - sunset date of July 2010
  - PEDs that were evaluated and approved under the Pre-PCI (Visa) PED program
  - PEDs evaluated and approved under the PCI program
- **Proposed sunset only affects Pre-PCI attended POS PEDs**
  - Pre-PCI PEDs approved between April 2002 - December 2004
  - Pre-PCI PED approvals for new deployments expired December 2007
- **Tentative target date - December 2014**
  - Allows approximately seven years from the approval expiration
  - Accommodates the natural expiration of most of PEDs
- **See Visa PED FAQ on [www.visa.com/cisp](http://www.visa.com/cisp)**
  - Visa Europe announced Pre-PCI attended POS PED expiration - December 2012
  - Visa Inc. will announce shortly



# Known Compromised PEDs

*NOTE:* For the most recent list of known compromised PEDs see Bulletin on [www.visa.com/cisp](http://www.visa.com/cisp)

## **Vendor Attested**

### **VeriFone**

- PINpad 101
- PINpad 201
- PINpad 2000
- Everest

### **Hypercom**

- S7S
- S8

### **Ingenico**

- eN-Crypt 2400
- C2000 Protégé

**Compromised PEDs are listed on [www.visa.com/cisp](http://www.visa.com/cisp)**

**Nov. 2007 Visa Security Alert “POS PIN Entry Device Vulnerabilities”**

**All Vendor attested attended POS PEDs (neither pre-PCI or PCI approved) must be removed from production by July 1, 2010**

**Recently a Pre-PCI attended POS PED was identified as compromised:**

**Ingenico eN-Crypt 2100**

# TDES / PED Best Practices and Requirements

## Best Practices:

- Use PCI PED V2 PEDs - tested under more robust standards
- Touch PEDs once - if PED being repaired, use opportunity to redeploy with TDES keys
- Use PED's key registers to load future use TDES keys
- Retire compromised PEDs ASAP
- If available, use PCI UPT and PCI HSM approved devices

## Requirements:

- Generate a new Base Derivation Key (BDK) for TDES DUKPT implementations (PCI PIN Requirement 19)
  - SDES DUKPT BDK must not be used for TDES
- Only use Interlink ESOs that have been registered with Visa



# For More PIN Security Information



**[www.visa.com/cisp](http://www.visa.com/cisp)**

- *April 2009 Update on Visa's TDES Policy*
- *NEW: Visa US POS TDES Frequently Asked Questions*
- *Visa PED Frequently Asked Questions*
- *Visa PIN Security Tools and Best Practices for Merchants*
- *PCI PIN Security Requirements v2 Jan. 2008*
  - *Visa specific requirements - Annex A*
- *Visa PIN Security Program: Auditor's Guide*
- *PIN Security Training registration information*
- *Compromised POS PED Bulletin*
- *Other PIN security related Bulletins*

**[www.visa.com/pin](http://www.visa.com/pin)**

**[www.visa.com/pinsecurity](http://www.visa.com/pinsecurity)**

# Information on PCI PED Security Standards



## PCI Security Standards Council

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

- *PCI POS PIN Entry Device Security Requirements*
- *PCI EPP Security Requirements*
- *PCI UPT Security Requirements*
- *PCI HSM Security Requirements*
- PCI Approved PIN Entry Device List
  - 100 Vendors
  - 296 PEDs

# Visa Security Trainings and Webinars



## Visa One-Day Key Management Workshop:

- October 7, 2009 – Foster City, CA
- Go to [www.visa.com/cisp](http://www.visa.com/cisp) for more information
- North American Training Schedule to be announced
- Trainings are accredited for Continuing Professional Education
- Custom in-house training sessions available
- To register contact: [pinusa@visa.com](mailto:pinusa@visa.com)

## Visa Webinar for Franchise Operators

- September 29, 2009
- *Top 5 Data Security Trends Impacting Franchise Operators*
- For registration information contact [cisp@visa.com](mailto:cisp@visa.com)

## Final Thoughts on Fraud and PIN Security



Protecting the payment system is a shared responsibility for all payment system participants

Everyone has an important role to play:

- Issuers
- Acquirers
- Merchants
- Cardholders
- Processors
- Third Party Agents
- Public/Government Officials
- Law Enforcement

# Your PIN Security Contacts at Visa



Stoddard Lambertson  
650-432-1470  
stoddard@visa.com

Ross Snailer  
650-432-1764  
rsnailer@visa.com

pinusa@visa.com

Regional PIN Security Contacts in all Visa regions



# Questions

